A Provably Secure Ring Signature Scheme in Certificateless Cryptography*

Lei Zhang[1], Futai Zhang[1], and Wei Wu[2]

[1]College of Mathematics and Computer Science
Nanjing Normal University, P.R. China
[2]Centre for Computer and Information Security Research
School of Computer Science & Software Engineering
University of Wollongong, Australia
lei_zhangzl@126.com, zhangfutai@njnu.edu.cn,
weiwu81@gmail.com

Abstract. Ring signature is a kind of group-oriented signature. It allows a member of a group to sign messages on behalf of the group without revealing his/her identity. Certificateless public key cryptography was first introduced by Al-Riyami and Paterson in Asiacrypt 2003. In certificateless cryptography, it does not require the use of certificates to guarantee the authenticity of users' public keys. Meanwhile, certificateless cryptography does not have the key escrow problem, which seems to be inherent in the Identity-based cryptography. In this paper, we introduce the notion of ring signature into certificateless public key cryptography and propose a concrete certificateless ring signature scheme. The security models of certificateless ring signature are also formalized. Our new scheme is provably secure in the random oracle model, with the assumption that the Computational Diffie-Hellman problem is hard.

Keywords: Ring Signature, Certificateless Cryptography, Provable Security, Random Oracle model.

1 Introduction

In Asiacrypt 2001, Rivest, Shamir and Tauman [26] introduced the concept of ring signature, which makes it possible to specify a set of possible signers without revealing which member actually produced the signature. As pointed in [26], ring signatures provide an elegant way to leak authoritative secrets in an anonymous way, to sign casual email in a special way that can only be verified by its intended recipient, anonymous membership authentication for ad hoc groups [6], etc. In addition, ring signatures can also be served as the building block of concurrent signatures and solve some other problems in multiparty computations.

Certificateless public key cryptography (CL-PKC) is a new paradigm proposed by Al-Riyami and Paterson [2]. It enjoys the implicit certification property of

* Project supported by the nature science foundation of China (No. 60673070), the nature science foundation of Jiangsu province (No. BK2006217).

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 103–121, 2007.

identity based public key cryptography (ID-PKC) [27] while without suffering from its inherent key escrow problem. Different from ID-PKC, a third party which we call Key Generation Center (KGC) in CL-PKC does not have access to a user's private key. Instead, the KGC supplies a user with a partial private key, which derives from the user's identity. Then the user combines the partial private key with some secret information chosen by himself to generate his actual private key. The corresponding public key is computed from the system's public parameters and the secret information chosen by the user, and is published by the user himself. Like ID-PKC, CL-PKC does not use public key certificates. The KGC does not access the full private key of a user, hence, certificateless cryptography does not suffer from the key escrow problem.

In this paper, we integrate the concept of ring signatures with certificateless cryptography to give the notion of certificateless ring signatures (CL-Ring), and investigate secure and efficient construction of CL-Ring schemes.

Motivations. Certificateless cryptography have some advantages over traditional PKC and ID-PKC in some aspects. As a useful primitive, ring signatures have been studied in traditional PKC and ID-PKC for more than five years. Even in a theoretic point of view, ring signatures should be studied in CL-PKC to rich the theories and techniques of CL-PKC. In practice, to generate a ring signature on behalf of a group in traditional PKC, the signer must first verify all the certificates of the group members, otherwise his anonymity is jeopardized and the ring signature will be rejected if he uses invalid certificates of some group members. Given a ring signature, the verifier must perform the same verification as well before checking the validity of the ring signature. These verifications inevitably lead to the inefficiency of the whole scheme since the computational cost increases linearly with the group size. Although Identity-based ring signatures eliminate such costly verifications, they suffer from a security drawback induced by the inherent key escrow problem of ID-PKC. Namely, a malicious PKG can always issue valid ring signatures on behalf of any group. As CL-PKC does not use public key certificates, and in the meantime, it removes the key escrow problem of ID-PKC, we think it supplies an appropriate environment for implementing ring signatures. So it is necessary to extend the notion and security model of ring signatures to CL-PKC. Compared with ring signature schemes in traditional PKC, in a CL-Ring scheme, both the signer and the verifier can avoid the costly verification of group members' certificates. On the other hand, in contrast to ID-based ring signatures, the KGC can no longer forge a ring signature on behalf of a group without being detected.

In application aspects, like ring signatures in traditional PKC and ID-PKC, certificateless ring signatures can also be used in leaking authoritative secrets in an anonymous way, anonymous membership authentication for ad hoc groups [6], reports to the authorities embezzlement and corruption, certificateless designated signatures and concurrent signatures, etc.

Our Contributions. In this paper, we introduce the notion of ring signature into certificateless cryptography and propose a concrete certificateless ring signature scheme.